AMENDMENTS TO CLAIMS

The following listing of the claims replaces all prior claim versions and listings.

1. (Canceled)

2. (Currently Amended) A method of calculating a value of a given function by using an apparatus including a plurality of computers, comprising:

an input process;

an ElGamal cipher text preparation process;

a sequential substitution reencryption process; and

a result output process,

characterized in that the input process comprises an information input step of inputting to the plurality of computers information on a circuit including a plurality of gates and the information ~~on the plurality of computers~~, and a dispersion input step of inputting to each of the computers each one of plural pieces of partial data which are obtained by dispersing input data of the given function into plural pieces by the number of the computers,

the ElGamal cipher text preparation process comprises an ElGamal cipher text preparation step ~~of generating~~ in which at least one of the computers generates a set of ElGamal cipher texts ~~in which at least one of the computers corresponds~~ corresponding to inputs of the [[gate]] gates of the circuit that realizes the given function,

the sequential substitution reencryption process comprises a step of allowing each of the computers to perform a substitution reencryption process one after another, and the substitution reencryption process comprises a cipher text obtaining step of allowing the computer in [[this]] turn to receive the set of ElGamal cipher texts from the computer in the previous turn, a cipher

text substitution and reencryption step of changing an order of the set of ElGamal cipher texts received in the cipher text obtaining step for substitution and subjecting those cipher texts to reencryption, [[and]] a step of disclosing the data generated in the cipher text substitution and reencryption step to at least the computer in [[the]] next order, and a step of stopping the sequential substitution reencryption process when all of the computers have performed the sequential substitution reencryption process, and

the result output process comprises a partial decryption step of deciphering or partially deciphering a part of the cipher texts generated in the cipher text substitution and reencryption step, a decryption step of deciphering a cipher text that enciphers data corresponding to the input to the circuit in the cipher texts generated in the cipher text substitution and reencryption step, and an evaluation step of evaluating an output of the circuit by using the data deciphered in the decryption step and the data partially deciphered in the partial decryption step.

3. (Currently Amended) A calculation system for evaluating a function, comprising:

a plurality of computers;

communication means for performing communication with the plurality of computers;

input process means;

ElGamal cipher text preparation means;

sequential substitution reencryption means; and

result output means,

characterized in that the input means inputs information on a circuit whose output is desired to be obtained, information on the plurality of computers, and information on which part of an input to the circuit each of the computers has,

the ElGamal cipher text preparation means prepares ElGamal cipher texts for generating a set of ElGamal cipher texts corresponding to inputs of gates of the circuit that realizes the ~~given~~ function,

the sequential substitution reencryption means comprises cipher text obtaining means for allowing the computer in [[this]] turn to receive the set of ElGamal cipher texts from the computer in the previous turn, cipher text substitution and reencryption means for changing an order of the set of ElGamal cipher texts received by the cipher text obtaining means for substitution and subjecting those cipher texts to reencryption, [[and]] means for disclosing the data generated by the cipher text substitution and reencryption means to at least the computer in [[the]] next order, and means for stopping operation of the sequential substitution reencryption means when the sequential substitution reencryption means has been performed with all of the computers, and

the result output means comprises partial decryption means for deciphering or partially deciphering a part of the cipher texts generated by the cipher text substitution and reencryption means, decryption means for deciphering encryption related to itself of a cipher text that enciphers data corresponding to the input to the circuit in the cipher texts generated by the cipher text substitution and reencryption means, and evaluation means for evaluating an output of the circuit while using the data deciphered by the decryption means by the plurality of computers and the data partially deciphered by the partial decryption means by the plurality of computers.

4. (Currently Amended) The calculation method according to Claim 2,

characterized in that the set of ElGamal cipher texts corresponding to [[each]] the inputs of the gates is a set of ElGamal cipher texts of a secret key, corresponding to each of the inputs

of the gates, generated ~~corresponding to each of the gate~~ by each of the computers, and

a public key used for generating the ElGamal cipher texts is a sum of public keys corresponding to gates for generating two ~~signals input~~ signal inputs to [[this]]the gate.

5. (Currently Amended) The calculation method according to Claim 2,

characterized in that the input process further comprises a step of inputting an area variable of an ElGamal encryption method to each of the computers,

the ElGamal cipher text preparation process further comprises a gate secret key generating step of generating a secret key of the ElGamal cipher texts corresponding to [[each]] the inputs of the gates of the circuit by each of the computers,

each of the computers performs:

a gate public key generating step of generating a gate public key corresponding to the secret key generated in the gate secret key generating step;

a gate public key validity proof generating step of generating a gate public key validity proof for the public key generated in the gate public key generating step;

a gate public key validity proof disclosing step of disclosing the gate public key validity proof generated in the gate public key validity proof generating step;

an input gate secret key generating step of generating a secret key of the ElGamal cipher texts corresponding to ~~a gate~~ the inputs of the gates where an input is directly made to the circuit of the gates of the circuit;

an input gate public key generating step of generating an input gate public key corresponding to the secret key generated in the input gate secret key generating step;

an input gate public key validity proof generating step of generating a validity proof for

the input gate public key generated in the input gate public key generating step;

an input gate public key validity proof disclosing step of disclosing the input public key validity proof generated in the input gate public key validity proof generating step;

a gate public key obtaining step of obtaining gate public keys generated by other respective computers;

a gate public key integration step of integrating the gate public keys obtained in the gate public key obtaining step;

a gate public key encryption step of enciphering the gate secret key cipher text ~~generated by this computer~~ with the gate public key integrated in the gate public key integration step;

a gate secret key cipher text disclosing step of disclosing a gate secret key cipher text generated in the gate public key encryption step;

a gate secret key cipher text validity proof generating step of generating a validity proof for the gate secret key cipher text;

a gate secret key cipher text validity proof disclosing step of disclosing the gate secret key cipher text validity proof generated in the gate secret key cipher text validity proof generating step;

an input cipher text generating step of generating a cipher text corresponding to a part of the input [[of]] to the circuit that is input to each of the computers[[.]];

an input cipher text validity proof generating step of generating a validity proof for the cipher text corresponding to the part of the input of the circuit generated in the input cipher text generating step;

an input cipher text validity proof disclosing step of disclosing the proof generated in the input cipher text validity proof generating step; and

an output cipher text generating step of generating and disclosing a cipher text corresponding to an output of the gate,

the sequential substitution reencryption process comprises:

a gate secret key cipher text substitution and reencryption step of changing an order of a set of the gate secret key cipher texts with one substitution randomly selected on the basis of a predetermined permitted substitution method for reencryption;

an input cipher text substitution and reencryption step of changing an order of a set of the input cipher texts with one substitution randomly selected on the basis of a predetermined permitted substitution method for reencryption;

an output cipher text substitution and reencryption step of changing an order of a set of the output cipher texts with one substitution randomly selected on the basis of a predetermined permitted substitution method for reencryption; and

a gate secret key cipher text, input cipher text, and output cipher text substitution and reencryption validity proof generating and disclosing step of generating and disclosing validity proofs for the substitution and reencryption performed in the gate secret key cipher text substitution and reencryption step, the input cipher text substitution and reencryption step, and the output cipher text substitution and reencryption step,

the partial decryption step of the result output process comprises:

a gate secret key partial decryption step of partially deciphering the gate secret key cipher texts by mutually performing communication and calculation by the computers;

an input cipher text partial decryption step of partially deciphering the input cipher texts by mutually performing communication and calculation by the computers;

an output cipher text partial decryption step of partially deciphering the output cipher

texts by mutually performing communication and calculation by the computers; and

a gate secret key, input cipher text, and output cipher text partial decryption step validity proof generating and disclosing step of generating and disclosing the validity proofs for the partial decryption performed in the gate secret key partial decryption step, the input cipher text partial decryption step, and the output cipher text partial decryption step, and

the calculation method further comprises a step of verifying various validity proofs disclosed by other computers.

6. – 10. (Canceled)